UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/629,170	07/29/2003	Bruce Wallman	CHA920030012US1	7168

23550 7590 05/29/2008

HOFFMAN WARNICK LLC
75 STATE STREET
14TH FLOOR
ALBANY, NY 12207

EXAMINER	
TESLOVICH, TAMARA	

ART UNIT	PAPER NUMBER
2137	

NOTIFICATION DATE	DELIVERY MODE
05/29/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTOCommunications@hwdpatents.com

Office Action Summary	Application No.	Applicant(s)	
	10/629,170	WALLMAN, BRUCE	
	Examiner	Art Unit	
	Tamara Teslovich	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 January 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to the Applicant's Remarks filed January 25, 2008.

Claims 4 and 12 are amended.

Claims 1-22 are pending and herein considered.

Response to Arguments

Applicant's amendments to claims 4 and 12 serve to overcome the Examiner's previously set forth 35 USC 112 rejections of claims 4 and 12 as indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as his invention. The 35 USC 112 rejections of claims 4 and 12 have been withdrawn.

Applicant's arguments in response to the Examiner's rejections of claims 1-22 have been considered but are not persuasive.

Regarding Applicant's remarks concerning Ollman's alleged failure to disclose a system for detecting improper requests as claimed in claim 1, the Examiner respectfully disagrees. First, the Examiner would like to remind Applicant that cited portions of the reference have been included to direct Applicant's attention to those portions of the reference the Examiner considers most pertinent. Those citations are not meant to limit the reference in any way; it is the reference in its entirety that has been used to reject Applicant's claims. Furthermore, the Examiner is unsure exactly how it is that a system such as Ollmann's which has been designed to deal with unexpected or "error" requests

could possible fail to include a system for detecting those requests. The Examiner is aware of no such system that includes the second part without the first. Even so, the Examiner would like to draw attention to a number of portions of the Ollmann including "A Standard HTML Authentication Form" on pages 2-3 disclosing the use of "authentication procedures" used to detect improper requests "client-side" and "server-side" "data validations" to detect improper requests. On page 4, Ollmann goes on to describe the ability of the application to track and log connections related to the source IP address of the web client in order to identify authentication failures to multiple user accounts by a single IP address and take those actions appropriate. These portions of the reference are just a few of the many portions which clearly teach Ollmann's ability to detect improper requests in order that it may respond to such requests. It is based upon these arguments and the reference in its entirety that the Examiner maintains her rejection of claim 1 in view of Ollmann.

Regarding Applicant's remarks concerning Ollman's alleged failure to disclose a "wherein the system for responding stops issuing HTTP "OK" response codes and issues no response after a predetermined number of improper requests are detected" as claimed in claim 2, the Examiner respectfully disagrees. Applicant sites to portions of page 4 which call for the automatic lockout with further attempts generating the same failure message. Applicant however fails to mention the paragraph directly below that quoted:

> "Again, automatically lockout an account after a threshold has been reached (e.g. three authentication failures), and do not inform the client system that this process has happened." (page 4 lines 12-14)

It is clear from the above cited portion that Ollmann does in fact teach wherein the system for responding stops issuing HTTP "OK" response codes and issues no response after a predetermined number of improper requests are detected. Applicant argues that a "lockout" is different from "stopping the issuance of responses" however, such an argument is wholly unsupported, and furthermore, inconsistent with Ollmann's teachings. The Examiner maintains her rejection based on the above made arguments and in view of the reference in its entirety insofar as she believes that Ollmann's "lockout" and consequent "do not inform the client" "after a threshold has been reached" amounts to Applicant's "stops issuing HTTP "OK"" and "issues no response after a predetermined number of improper requests."

Regarding Applicant's remarks concerning Ollman's alleged failure to disclose a "wherein a request is deemed improper if a message body associated with the request has zero length" as claimed in claim 4, the Examiner respectfully disagrees. First, the Examiner would like to point out that the limitation argued by Applicant is newly added, and as such, there is no way that the Examiner could have argued it in her last action. Second, the Examiner would like to draw attention to portions of both the Ollmann and W3C references that teach the limitation in question. First, the Examiner would like to draw attention to page 8 of the primary reference wherein Ollman clearly discloses ensuring that content

is "of the expected size and type." Furthermore, the Examiner would like to point out those numerous portions of the W3C reference, including but not limited to page 10, wherein the reference teaches the use of checks to determine the types of packets received and rejecting those packets that are merely empty packets being used to overwhelm a target or those sent to communication between agents and masters. It is clear from these portions in view of the two references in their entirety that the combined system of Ollmann and W3C disclose the categorization of requests as improper when they are of the wrong type or fail to include a body, suggesting that they are invalid and merely being used to overwhelm a system.

Regarding Applicant's remarks concerning Ollman's alleged failure to disclose a "wherein a request is deemed improper if an HTTP "post" or an HTTP "get" command is expected and neither an HTTP "post" nor an HTTP "get" command is received" as claimed in claim 5, the Examiner respectfully disagrees. The Examiner would like to draw attention first and foremost to the primary reference wherein Ollmann discloses in particular the use of post and get commands by programmers throughout the reference, and particularly on page 3. Next the Examiner would like to point out those sections of the reference that utilize authentication and authorization checks designed to examine each incoming packet and refuse access for any packet that fails to be the proper type and size. In reference to those portions of the W3C reference cited by the Examiner and mentioned by Applicant, the Examiner has included those portions to show the diverse ways in which the W3C system determines a request

improper as the result of its type. In particular page 10 points out a number of particular packet types that should be refused access including but not limited to echo request and reply packets, ICMP echo messages, UDP packets, and particular reply packets according to the their content. It is clear from these portions in view of the two references in their entirety that the combined system of Ollmann and W3C disclose the categorization of requests as improper when basic HTTP "post" and "get" commands are expected by a system, but neither are received.

Regarding Applicant's remarks concerning Ollman's alleged failure to disclose a "wherein the system for responding to improper requests includes a response protocol that utilizes a standard error handling procedure for a first improper request from a requesting resources, issues an HTTP OK response code for N subsequent improper requests from the requesting resource, and then stops responding to the requesting resource altogether" as claimed in claim 88, the Examiner respectfully disagrees. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. Applicant's arguments amount to a listing of claim limitations and an allegation that they are not taught within the reference. Addressing Applicant's first limitation, there is no question that the reference at hand teaches a "system for responding to improper requests including a response protocol that utilizes a standard error handling procedure for a first improper request from a requesting resource" insofar as

Ollman teaches the use of standard error handling procedures for responding to improper requests, supplemented by procedures tailored to protecting against DOS attacks and the likes. Support for such a contention may be found throughout the reference, and in particular on page 2 wherein Ollmann discloses General "Authentication Failure" messages to be presented to improper requests. Moving on to Applicant's next limitation, the Examiner maintains her position that Ollmann teaches the issuance of HTTP "OK" response code for N subsequent improper requests from the requesting resource. Support for the Examiner's position may be found on page 5 wherein Ollmann discloses the use of "HTTP 200 OK" responses instead of 400 type errors. The last limitation argued by Applicant regarding wherein the system "stops responding to the requesting resource altogether "after N subsequent improper requests from the requesting source" mirrors that limitation argued above with respect to claim 2. The Examiner refers Applicant to those arguments and citations provided above in support of Ollmann's teaching of issuing "no response after a predetermined number of improper requests." It is based upon the above made arguments in view of the Ollmann reference in its entirety that the Examiner maintains her position that Ollmann anticipates each and every limitation of claim 8.

Regarding Applicant's remarks concerning claims 10 and 17 and their recitation to a process similar to that discussed with respect to claim 8, the Examiner respectfully maintains her position for those reasons given above with regards to claim 8.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1-4, 7-12, and 15-22 are rejected undyou're er 35 U.S.C. 102(a) as being anticipated by Gunter Ollmann's Custom HTML Authentication – Best Practices on Securing Custom HTML Authenitcation Procedures, hereinafter referred to as *Ollmann*.

As per **claim 1**, Ollmann teaches a system for addressing denial of service attacks directed at a web resource, comprising a system for detecting improper requests; and a system for responding to improper requests that issues an HTTP "OK" response code when improper request is detected (page 5).

As per **claim 2,** Ollmann teaches wherein the system for responding stops issuing HTTP "OK" response codes and issues no response after a predetermined number of improper requests are detected (page 4 line 6 "automatically lockout after a threshold has been reached (e.g. three authentication failures)").

As per **claim 3**, Ollmann teaches wherein a request is deemed improper if the request is received from an unexpected host (page 4 line 35 "it may be possible to dynamically block an offending IP address" and line 32 "the web-based application must be able to track and log connections relating to the source IP address of the web client").

As per **claim 4**, Ollmann teaches wherein a request is deemed improper if a message body associated with the request has a zero length (pages 4-5).

As per **claim 7**, Ollmann teaches wherein the HTTP "OK" response code comprises an HTTP 204 "OK" message code (pages 4-5).

As per **claim 8**, Ollmann teaches wherein the system for responding to improper requests includes a response protocol that utilizes a standard error handling procedure for a first improper request from a requesting resource, issues an HTTP OK response code for N subsequent improper requests from the requesting resource, and then stops responding to the requesting resource altogether (page 4 line 6 "automatically lockout after a threshold has been reached (e.g. three authentication failures)").

As per **claim 9**, Ollmann teaches wherein the web resource comprises a server (pages 1-3).

As per **claim 10**, Ollmann teaches a method for addressing denial of service attacks directed at a web resource (page 5), comprising: receiving messages at the web resource; analyzing each message and determining if the message is improper; storing the source address of a message if the message is improper (pages 1-5); responding to a first improper message from an identified

source address with an HTTP error response; responding to a set of subsequent improper messages from the identified source address with HTTP "OK" response codes (page 5); and stopping responses to the identified source address for all received improper messages after the set of subsequent improper messages have been responded to (page 4 line 6 “automatically lockout after a threshold has been reached (e.g. three authentication failures)”).

As per **claim 11**, Ollmann teaches wherein a message is deemed improper if the message is received from an unexpected host (page 4 line 35 “it may be possible to dynamically block an offending IP address” and line 32 “the web-based application must be able to track and log connections relating to the source IP address of the web client”).

As per **claim 12**, Ollmann teaches wherein a message is deemed improper if a message body associated with the request has a zero length (pages 4-5).

As per **claim 15**, Ollmann teaches wherein the HTTP "OK” response code comprises an HTTP 204 "OK" message code (pages 4-5).

As per **claim 16**, Ollmann teaches wherein the HTTP "OK” response comprises an HTTP 200 "OK" message code (pages 4-5).

As per **claim 17**, Ollmann teaches a program product stored on a recordable medium for addressing denial of service attacks directed at a web resource, comprising means for receiving messages at the web resource; means for analyzing each message and determining if the message is improper; means for storing the source address of a message if the message is improper (page 4

line 32 "the web-based application must be able to track and log connections relating to the source IP address of the web client. The application should be able to identify authentication failures to multiple user accounts initiated by a single IP address"); means for responding to a first improper message from an identified source address with an HTTP error response; and means for responding to subsequent improper messages from the identified source address with HTTP "OK" response codes (page 4 line 6 "automatically lockout after a threshold has been reached (e.g. three authentication failures)").

As per **claim 18**, Ollmann teaches means for stopping responses to the identified source address after a predetermined number of subsequent improper messages have been received (page 4 line 6 "automatically lockout after a threshold has been reached (e.g. three authentication failures)").

As per **claim 19**, Ollmann teaches wherein a message is deemed improper if the message is received from an unexpected host; if the message has a zero length; if the message is neither an expected HTTP "post" nor an expected HTTP "get" command; or if the message includes a HTTP "post" or "get" command with unknown arguments (page 4 line 35 "it may be possible to dynamically block an offending IP address" and line 32 "the web-based application must be able to track and log connections relating to the source IP address of the web client").

As per **claim 20**, Ollmann teaches wherein the HTTP "OK" response codes comprise HTTP 204 "OK" response codes (pages 4-5).

As per **claim 21**, Ollmann teaches wherein messages that are deemed proper are passed to the web resource for further processing (pages 3-4).

As per **claim 22**, Ollmann teaches wherein the web resource is a web server (pages 1-3).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims **5, 6, 13, and 14** are rejected under 35 U.S.C. 103(a) as being unpatentable over Gunter Ollmann's Custom HTML Authentication – Best Practices on Securing Custom HTML Authenitcation Procedures ("Ollmann") as applied to claims 1-4, 7-12, and 15-22 above, and further in view of The World Wide Web Seucirty FAQ Number 8 entitled "Securing against Denial of Service Attacks" ("W3C").

As per **claim 5**, Ollmann fails to teach wherein a request is deemed improper is an HTTP "post" or HTTP "get" command is expected and neither an HTTP "post" nor an HTTP "get" command is received.

W3C teaches wherein a request is deemed improper if an HTTP "post" or HTTP "get" command is expected and neither an HTTP "post" nor an HTTP "get" command is received (page 10).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Ollmann's system the ability to deem a request improper when an HTTP post or get is expected and neither is received as described in W3C to provide for a more secure system protected against attacks such as trinoo, tfn2k and other attacks that are known to utilize alternate packets.

As per **claim 6**, Ollmann fails to teach wherein a request is deemed improper if the request includes a HTTP "post" or "get" command with unknown arguments.

W3C teaches wherein a request is deemed improper if the request includes a HTTP "post" or "get" command with unknown arguments (page 10).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Ollmann's system the ability to deem a request improper when an HTTP post or get is received with unknown arguments as described in W3C to provide for a more secure system protected against attacks such as trinoo, tfn2k and other attacks that are known to utilize packets with unknown arguments.

As per **claim 13**, Ollmann fails to teach wherein a request is deemed improper is an HTTP "post" or HTTP "get" command is expected and neither an HTTP "post" nor an HTTP "get" command is received.

W3C teaches wherein a request is deemed improper if an HTTP "post" or HTTP "get" command is expected and neither an HTTP "post" nor an HTTP "get" command is received (page 10).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Ollmann's system the ability to deem a request improper when an HTTP post or get is expected and neither is received as described in W3C to provide for a more secure system protected against attacks such as trinoo, tfn2k and other attacks that are known to utilize alternate packets.

As per **claim 14**, Ollmann fails to teach wherein a request is deemed improper if the request includes a HTTP "post" or "get" command with unknown arguments.

W3C teaches wherein a request is deemed improper if the request includes a HTTP "post" or "get" command with unknown arguments (page 10).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Ollmann's system the ability to deem a request improper when an HTTP post or get is received with unknown arguments as described in W3C to provide for a more secure system protected

against attacks such as trinoo, tfn2k and other attacks that are known to utilize packets with unknown arguments.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865.

The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

T. Teslovich

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137